PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341262
(43)Date of publication of application : 08.12.2000

(51)Int.Cl. H04L 9/08
H04L 12/28

(21)Application number : 11-146698
(22)Date of filing : 26.05.1999

(71)Applicant : ADTEC:KK
(72)Inventor : FUJII SHIN

(54) RADIO TRANSMISSION DEVICE AND SETTING METHOD FOR KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To improve secrecy maintainability of key information by generating and storing a key and transferring the key to other radio transmission devices when a station is specified as a master station at the start of a key setting mode, and receiving and storing a key when specified as a slave station.
SOLUTION: Radio transmission devices 20 to 22 are equipped with ports for LAN connection using a hub (HAB) of, for example, 100 BASE-TX. The LAN ports of the radio transmission device 20 to 22 are connected to a hub 25 through LAN cables. A radio transmission device (e.g. 20) specified as a master station among the radio transmission devices 20 to 22 generates random common key information with its internal program, stores the key in its station, and transfer common key information to the radio transmission devices 21 and 22 specified as other slave stations through the hub 25. The format of transfer of the key is previously specified and unique. A slave station stores the received key in itself and ends the process.

LEGAL STATUS

[Date of request for examination] 26.05.1999

[Date of sending the examiner's decision of rejection] 09.01.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]	
[Patent number]	3592580
[Date of registration]	03.09.2004
[Number of appeal against examiner's decision of rejection]	2001-001512
[Date of requesting appeal against examiner's decision of rejection]	06.02.2001
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] In the radio-transmission equipment possessing a wireless data transceiver means, a key storage means to store a key in the storage means of a non-volatile, and an encryption means to perform a data encryption decryption using a key A key generation means, a key setting-out mode starting means, parents / child assignment means, and a cable data transceiver means, A key transfer means to transmit a key to other radio-transmission equipments using said cable data transceiver means, When key setting-out mode is started by key receiving means to receive a key using said cable data transceiver means, and said key setting-out mode starting means When specified as the key station by said parents / child assignment means While said key generation means generates a key and storing a key in the storage means of a non-volatile with said key storage means When a key is transmitted to other radio-transmission equipments with said key transfer means and it is specified as the child office by said parents / child assignment means Radio-transmission equipment characterized by having the key setting-out control means which receives a key with said key receiving means, and stores a key in the storage means of a non-volatile with said key storage means.

[Claim 2] Said cable data transceiver means is radio-transmission equipment according to claim 1 characterized by being a LAN interface circuitry.

[Claim 3] The 2nd process which sets other radio-transmission equipments except the 1st process which makes cable connection of two or more radio-transmission equipments which should set up a key, and one set made into a key station as a child office, starts key setting-out mode, and is changed into the waiting state waiting for receiving of a key, The setting-out approach of the key in radio-transmission equipment including the 3rd process transmitted to a child office through said cable connection while setting the radio-transmission equipment made into a key station as a key station, starting key setting-out mode, generating a key and storing a key in a

local station.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to the setting-out approach of the cryptographic key in the radio-transmission equipment used in the wireless LAN in a building, the data transmission between buildings, etc. about radio-transmission equipment.
[0002]
[Description of the Prior Art] Conventionally, when a transmission data encryption was performed in the radio-transmission equipment of the data used in the wireless LAN in a building, the data transmission between buildings, etc., the common key data of the secrecy used for encryption needed to be set as each radio-transmission equipment. Drawing 5 is the block diagram showing the common key setting-out approach in conventional radio-transmission equipment. For example, when a common key was set as radio-transmission equipment 10, the common key information which radio-transmission equipment 10 connected the terminal 13 to LAN connected, for example, the user determined was transmitted to radio-transmission equipment 10 from this terminal 13. In order to set a key as two or more radio-transmission equipments 10-12, the terminal 13 was connected to LAN to which each radio-transmission equipment is connected, and setting-out actuation of a key was performed, respectively.
[0003]
[Problem(s) to be Solved by the Invention] In conventional radio-transmission equipment which was described above Since setting out of a key is possible from the usual terminal and it reset up any number of times For example, there was a trouble that a communication link will be able to be intercepted, without accessing partner equipment in any way, when radio-transmission equipment 11 and radio-transmission equipment 12 were performing the encryption communication link and the same common key as near radio-transmission equipment 10 was set up. Moreover, even when a key was unknown, there was also a trouble that there was a possibility that a key may be decoded, by repeating key data in order and setting them up. The object of this invention solves the trouble of the above conventional techniques, and is to offer the radio-transmission equipment whose security-protection nature of key information improves.
[0004]

[Means for Solving the Problem] In the radio-transmission equipment with which this invention possesses a wireless data transceiver means, a key storage means to store a key in the storage means of a non-volatile, and an encryption means to perform a data encryption decryption using a key A key generation means, a key setting-out mode starting means, parents / child assignment means, and a cable data transceiver means, A key transfer means to transmit a key to other radio-transmission equipments using said cable data transceiver means, When key setting-out mode is started by key receiving means to receive a key using said cable data transceiver means, and said key setting-out mode starting means When specified as the key station by said parents / child assignment means While said key generation means generates a key and storing a key in the storage means of a non-volatile with said key storage means When a key is transmitted to other radio-transmission equipments with said key transfer means and it is specified as the child office by said parents / child assignment means, said key receiving means receives a key and it is characterized by having the key setting-out control means which stores a key in the storage means of a non-volatile with said key storage means.

[0005] Since according to this invention it is necessary to make cable connection of the equipment which should be set up by LAN etc. to set up a common key, it becomes difficult for those who are going to intercept after installing in a station etc. to perform common key setting-out processing. Moreover, since the radio-transmission equipment specified as the key station generates the common key information set up automatically and it transmits to a child office, even the contractor who sets a system, for example cannot know key information, but confidentiality improves. Since common key setting-out processing is redone in all radio-transmission equipments and new key information is set up when extending a child office, it is also difficult for a user to try decode of a key, and a possibility that a key may be decoded decreases.

[0006]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail. Drawing 1 is the block diagram showing the configuration of the communication system containing the radio-transmission equipment which applied this invention. In the example of drawing 1 , three radio-transmission equipments 20-22 are connected by the radio-transmission way. Each radio-transmission equipments 20-22 are connected to LAN, respectively, and two or more terminals and servers which are not illustrated are connected to each LAN. In order to encipher to each radio-transmission equipments 20-22, the common key information 23 which is 64-bit random data is stored, and each radio-transmission equipments 20-22 encipher transmission information using this key information, and decrypt the received encryption data.

[0007] Drawing 2 is the block diagram showing the system configuration for performing common key setting-out processing of this invention. Although it is

suitable for common key setting-out processing of this invention to bring together each radio-transmission equipments 20-22 in one place, and to carry them out before the contractor who builds a system installs each radio-transmission equipment in a service space, it is also possible to carry out, after arranging to an installation. Each radio-transmission equipments 20-22 are beforehand equipped with the port for LAN connection which uses hubs (HAB), such as 100BASE-TX. This LAN port is used in common key setting-out processing of this example. The LAN port of each radio-transmission equipments 20-22 is connected to a hub 25 with a LAN cable. And the radio-transmission equipment (for example, 20) specified as the key station of each radio-transmission equipments 20-22 transmits common key information to the radio-transmission equipments 21 and 22 specified as other child offices through the hub 25 while it generates random common key information and stores it in a local station by the internal program. The format which transmits a key is the unique thing specified beforehand. The key received in the child office is stored in a local station, and processing is ended.

[0008] Drawing 3 is the block diagram showing the configuration of the radio-transmission equipment of this invention. Radio-transmission equipment is connected with two or more terminals which are not illustrated through LAN of for example, a bus mold. The LAN interface circuitry 37 has the interface function of a signal with well-known bus formed LAN, receives the LAN packet addressed to other LANs based on control of CPU33, and stores it in the transmission buffer in RAM35. Moreover, it receives/decodes and the LAN packet addressed to self-LAN accumulated in the receive buffer in RAM35 is transmitted to LAN.

[0009] CPU33 controls the whole radio-transmission equipment based on the program stored in ROM34. That is, it enciphers based on common key information, it encodes to transmission, and the LAN packet in a transmission buffer is outputted through an interface circuitry 32. Moreover, a modulation code is decrypted for received data, a code is decrypted further, a LAN packet is reproduced, and it stores in the receive buffer in RAM35. When an error is detected by received data, CPU33 transmits a resending demand packet to partner equipment, and the partner equipment which received the resending demand packet resends the saved transmitting packet. A part of ROM [at least]34 is an electric target like a flash memory with the configuration which can be eliminated and written in, common key information is written in this part, and it is saved into it.

[0010] The transceiver circuit 31 builds in a sending circuit and a receiving circuit, and a sending circuit modulates a carrier based on the inputted data, and it changes, amplifies and outputs it to a predetermined frequency band. QAM etc. is arbitration and the modulation technique of a band is arbitrary. Moreover, a spectrum diffusion method may be adopted. A sending signal is transmitted from an antenna 30. The receiving circuit of the transceiver circuits 26-29 restores to it, decodes and outputs the signal received from the antenna 30. In addition, although it connects through the

attenuator, transmitted power is about several mW, and if transmission and the half-duplex which performs reception by turns are performed, a problem will not have a sending circuit and a receiving circuit.

[0011] The panel circuit 36 is an easy panel circuit for I/O which consists of for example, a DIP switch and a light emitting diode, the condition of a DIP switch is read by for example, the periodic target by CPU33, and the condition of equipment is displayed on a light emitting diode. It is used in order for one of DIP switches to start the common key setting-out mode of radio-transmission equipment, and other one is used in order to specify whether radio-transmission equipment is operated as a key station, or it is made to operate as a child office.

[0012] Drawing 4 is a flow chart which shows the content of common key setting-out processing of the radio-transmission equipment of this invention. This processing is periodically started by the timer. In S10, it is judged whether the DIP switch for starting the above mentioned common key setting-out mode is ON, and when a judgment result is affirmation, it shifts to S11. Although it is judged whether setting out of the DIP switch used in order to specify whether radio-transmission equipment is operated as a key station in S11 or it is made to operate as a child office is a key station, and it shifts to S12 when a judgment result is affirmation, in negation, it shifts S15.

[0013] When setting out is a key station, in S12, 64-bit random common key information is generated, using the program of the common knowledge which generates a value random whenever it starts, for example. In S13, it writes in and saves at the non-volatile ROM which described the generated key information above and which can be written in electric. In S14, the generated key information is transmitted from a LAN port in a unique predetermined format.

[0014] When setting out is a child office, in S15, it writes in and saves in waiting and S16 at the non-volatile ROM which described the received key information above and which can be written in until the LAN packet of the unique format in which key information was stored from the LAN port is received. Waiting and processing are ended until the DIP switch for starting the common key setting-out mode described above in S17 becomes off.

[0015] Next, the setting-out approach of a common key is explained with reference to drawing 2 . first, the radio-transmission equipments 20-22 which should set up a common key -- all LAN ports are connected to a hub 25. Next, the DIP switch for specifying whether the radio-transmission equipment in the panel circuit 36 is operated as a key station or it is made to operate as a child office only about one of the radio-transmission equipments 20-22 is set as a "key station." And this DIP switch of the other radio-transmission equipments 21 and 22 is set as a "child office."

[0016] Next, the DIP switch for starting the common key setting-out mode of the radio-transmission equipments 21 and 22 set as the "child office" is turned ON. Now,

the radio-transmission equipment of a "child office" will be in the standby condition of S15 of drawing 4 . The DIP switch for finally starting the common key setting-out mode of the radio-transmission equipment 20 set as the "key station" is turned ON. By this actuation, the radio-transmission equipment 20 of a "key station" performs processing of drawing 4 of S12-14, it transmits it to a child office while it generates and saves a common key, and it receives and stores key information in a child office.

[0017] By above configurations and actuation, the common key information on secrecy can be set as all radio-transmission equipments, without being indicated by not only a user but a manager and a maintenance man. In addition, in the common key setting-out approach of this invention, unless it starts common key setting-out mode in no radio-transmission equipments, a common key cannot be set up. If access to said DIP switch is forbidden by managing locking etc. only to the radio-transmission equipment which followed, for example, was set as the key station, even if it does not cope with it especially about the radio-transmission equipment of a child office, it is possible to prevent modification of a key.

[0018] As mentioned above, the following modifications are also considered by this invention although the example of this invention was indicated. In an example, although the example which sets up a common key using the LAN port used for a communication link was indicated, cable connection ports, such as dedication, for example, RS-232C etc., may be established in setting-out processing of a common key. In this case, a LAN port may be unnecessary if radio-transmission equipment has terminal capabilities. Moreover, since radio-transmission equipment possesses the radio link, it may use this radio link for common key setting-out processing.

[0019] Since unjust setting out can be prevented if only a key station is managed as described above, a key station may be equipped with the common key copy function which performs only S14 of drawing 4 , for example. In this case, the radio-transmission equipment of a child office and the radio-transmission equipment of a key station which are extended, for example are connected in a hub, the common key setting-out mode of a child office is started, and the common key copy processing described above in the key station is started. Then, a common key is transmitted to a child office from a key station, and a common key is stored in a child office. By the above processing, when extending radio-transmission equipment, the need of connecting all radio-transmission equipments in a hub is lost.

[0020] In addition, when the above copy functions are prepared, the DIP switch of a child office is changed, it considers as a key station, and reading a common key using a copy function is also considered. It follows, for example, the present parents / child setting-out information are also stored in the storage area of a common key, and when setting out is changed into a key station from a child office, the measures of eliminating the common key stored are taken.

[0021]

[Effect of the Invention] As stated above, when key setting-out mode is started by

the key setting-out mode starting means in radio-transmission equipment in this invention When specified as the key station by parents / child assignment means While a key generation means generates a key automatically and storing a key in the storage means of a non-volatile with a key storage means When a key is transmitted to other radio-transmission equipments and it is specified as the child office by the key transfer means Since it constituted so that a key receiving means might receive a key and a key might be stored in the storage means of a non-volatile with a key storage means, the key information to which even the contractor who sets a system, for example is set cannot be known, but it is effective in confidentiality improving.

[0022] Moreover, since according to this invention it is necessary to make cable connection of the radio-transmission equipment which should be set up by LAN etc. to set up a common key, it is effective in it becoming difficult for those who are going to intercept after installing in a station etc. to perform common key setting-out processing. Furthermore, since common key setting-out processing is redone in all radio-transmission equipments and new key information is set up when extending a child office, it is also effective in it being difficult and a possibility that a key may be decoded decreasing that a user tries decode of a key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of the communication system containing the radio-transmission equipment which applied this invention.

[Drawing 2] It is the block diagram showing the system configuration for performing common key setting-out processing of this invention.

[Drawing 3] It is the block diagram showing the configuration of the radio-transmission equipment of this invention.

[Drawing 4] It is the flow chart which shows the content of common key setting-out processing of the radio-transmission equipment of this invention.

[Drawing 5] It is the block diagram showing the common key setting-out approach in conventional radio-transmission equipment.

[Description of Notations]

10, 11, 12 [-- Common key information 25 / -- A hub, 30 / -- An antenna, 31 / -- A transceiver circuit 32 / -- An interface circuitry, 33 / -- CPU 34 / -- ROM 35 / -- RAM 36 / -- A panel circuit 37 / -- LAN interface circuitry] -- Radio-transmission equipment, 13 -- A terminal, 20, 21, 22 -- Radio-transmission equipment, 23

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－341262
（P2000－341262A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
12/28			６０１Ｅ	５Ｋ０３３
		11/00	３１０Ｂ	

審査請求　有　　請求項の数２　ＯＬ　（全６頁）

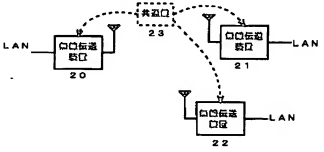
(21)出願番号　特願平11－146698
(22)出願日　平成11年５月26日(1999.5.26)

(71)出願人　596145916
株式会社　アドテック
東京都目黒区東山１丁目４番４号
(72)発明者　酌井　慎
京京都目黒区京山１－４－４目黒京山ビル
株式会社アドテック内
(74)代理人　100102336
弁理士　久保田　直樹

Ｆターム(参考)　5J104 AA01 AA16 EA16 EA21 JA03
NA02 NA37 PA00 PA07
5K033 AA08 CB01 CC04 DA01 DA17
DB12 EA07 EC01

(54)【発明の名称】　無線伝送装置および鍵の設定方法

(57)【要約】
【課題】鍵情報の機密保持性が向上する無線伝送装置を提供すること。
【解決手段】無線データ送受信手段、鍵記憶手段、暗号化手段を具備する無線伝送装置において、起動手段によって鍵設定モードが起動された場合に、親局に指定されている場合には、鍵生成手段によって鍵を生成し、鍵記憶手段によって鍵を記憶手段に格納すると共に、鍵転送手段によって鍵を他の無線伝送装置に転送する。また子局に指定されている場合には、鍵受信手段によって鍵を受信し、鍵記憶手段によって鍵を記憶手段に格納する。本発明によれば、共通鍵を設定する場合には装置をＬＡＮ等によって有線接続する必要があるので、盗聴しようとする者が共通鍵設定処理を実行することが困難となる。また、共通鍵は親局が自動的に生成し、子局へ転送するので、管理者でも鍵情報を知ることができず、機密性が向上する。



【特許請求の範囲】
【請求項１】無線データ送受信手段と、鍵を不揮発性の記憶手段に格納する鍵記憶手段と、鍵を使用してデータの暗号化復号化を行う暗号化手段とを具備する無線伝送装置において、
鍵生成手段と、
鍵設定モード起動手段と、
親／子指定手段と、
有線データ送受信手段と、
前記有線データ送受信手段を使用して鍵を他の無線伝送装置に転送する鍵転送手段と、
前記有線データ送受信手段を使用して鍵を受信する鍵受信手段と、
前記鍵設定モード起動手段によって鍵設定モードが起動された場合に、前記親／子指定手段により親局に指定されている場合には、前記鍵生成手段によって鍵を生成し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納すると共に、前記鍵転送手段によって鍵を他の無線伝送装置に転送し、前記親／子指定手段により子局に指定されている場合には、前記鍵受信手段によって鍵を受信し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納する鍵設定制御手段とを備えたことを特徴とする無線伝送装置。
【請求項２】前記有線データ送受信手段はＬＡＮインターフェイス回路であることを特徴とする請求項１に記載の無線伝送装置。
【請求項３】鍵を設定すべき複数の無線伝送装置を有線接続する第１の工程と、
親局とする１台を除く他の無線伝送装置を子局に設定し、鍵設定モードを起動して鍵の受信待ち状態にする第２の工程と、
親局とする無線伝送装置を親局に設定し、鍵設定モードを起動して鍵を生成し、鍵を自局に格納すると共に子局に前記有線接続を介して転送する第３の工程とを含む無線伝送装置における鍵の設定方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は無線伝送装置に関し、特にビル内の無線ＬＡＮやビル間のデータ伝送などにおいて使用される無線伝送装置における暗号鍵の設定方法に関するものである。
【０００２】
【従来の技術】従来、ビル内の無線ＬＡＮやビル間のデータ伝送などにおいて使用されるデータの無線伝送装置において、伝送データの暗号化を行う場合には、暗号化に使用する秘密の共通鍵データを各無線伝送装置に設定する必要があった。図５は、従来の無線伝送装置における共通鍵設定方法を示すブロック図である。例えば無線伝送装置１０に共通鍵を設定する場合には、端末１３を無線伝送装置１０が接続されているＬＡＮに接続し、例えば使用者が決定した共通鍵情報を該端末１３から無線伝送装置１０へ転送していた。複数の無線伝送装置１０～１２に鍵を設定するためにはそれぞれの無線伝送装置が接続されているＬＡＮに端末１３を接続してそれぞれ鍵の設定操作を行っていた。
【０００３】
【発明が解決しようとする課題】上記したような、従来の無線伝送装置においては、通常の端末から鍵の設定が可能であり、かつ何度でも設定し直すことができたので、例えば無線伝送装置１１と無線伝送装置１２とが暗号化通信を行っている場合に、近傍にある無線伝送装置１０に同じ共通鍵を設定すると、相手装置に何らアクセスすることなく、通信を盗聴できてしまうという問題点があった。また、鍵が不明な場合でも、鍵データを順に繰り返し設定することによって鍵が解読される恐れがあるという問題点もあった。本発明の目的は、前記のような従来技術の問題点を解決し、鍵情報の機密保持性が向上する無線伝送装置を提供することにある。
【０００４】
【課題を解決するための手段】本発明は、無線データ送受信手段と、鍵を不揮発性の記憶手段に格納する鍵記憶手段と、鍵を使用してデータの暗号化復号化を行う暗号化手段とを具備する無線伝送装置において、鍵生成手段と、鍵設定モード起動手段と、親／子指定手段と、有線データ送受信手段と、前記有線データ送受信手段を使用して鍵を他の無線伝送装置に転送する鍵転送手段と、前記有線データ送受信手段を使用して鍵を受信する鍵受信手段と、前記鍵設定モード起動手段によって鍵設定モードが起動された場合に、前記親／子指定手段により親局に指定されている場合には、前記鍵生成手段によって鍵を生成し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納すると共に、前記鍵転送手段によって鍵を他の無線伝送装置に転送し、前記親／子指定手段により子局に指定されている場合には、前記鍵受信手段によって鍵を受信し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納する鍵設定制御手段とを備えたことを特徴とする。
【０００５】本発明によれば、共通鍵を設定する場合には設定すべき装置をＬＡＮ等によって有線接続する必要があるので、職場等に設置した後に例えば盗聴しようとする者が共通鍵設定処理を実行することが困難となる。また、設定される共通鍵情報は親局に指定された無線伝送装置が自動的に生成し、子局へ転送するので、例えばシステムのセッティングを行う業者でさえも鍵情報を知ることができず、機密性が向上する。子局を増設する場合などには全ての無線伝送装置において共通鍵設定処理をやり直し、新たな鍵情報が設定されるので、使用者が鍵の解読を試みることも困難であり、鍵が解読される恐れが減少する。
【０００６】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。図１は、本発明を適用した無線伝送装置を含む通信システムの構成を示すブロック図である。図１の例においては３つの無線伝送装置２０～２２が無線伝送路によって接続されている。各無線伝送装置２０～２２はそれぞれＬＡＮに接続されており、各ＬＡＮには図示しない複数の端末やサーバが接続されている。各無線伝送装置２０～２２には暗号化を行うために、例えば６４ビットのランダムなデータである共通鍵情報２３が格納されており、各無線伝送装置２０～２２はこの鍵情報を使用して伝送情報を暗号化し、また受信した暗号化データを復号化する。

【０００７】図２は、本発明の共通鍵設定処理を実行するためのシステム構成を示すブロック図である。本発明の共通鍵設定処理は、例えばシステムを構築する業者が各無線伝送装置を使用場所に設置する前に、各無線伝送装置２０～２２を１カ所に集めて実施するのが好適であるが、設置場所に配置した後に実施することも可能である。各無線伝送装置２０～２２には予め、例えば100BASE-TX等のハブ（ＨＡＢ）を使用するＬＡＮ接続用のポートが装備されている。この実施例の共通鍵設定処理においてはこのＬＡＮポートを使用する。各無線伝送装置２０～２２のＬＡＮポートをＬＡＮケーブルによってハブ２５に接続する。そして、各無線伝送装置２０～２２の内の親局に指定された無線伝送装置（例えば２０）は内部のプログラムによってランダムな共通鍵情報を生成し、自局に格納すると共に、ハブ２５を介して他の子局に指定された無線伝送装置２１、２２に共通鍵情報を転送する。鍵を転送するフォーマットは予め指定されたユニークなものである。子局においては受信した鍵を自局に格納し、処理を終了する。

【０００８】図３は、本発明の無線伝送装置の構成を示すブロック図である。無線伝送装置は例えばバス型のＬＡＮを介して図示しない複数の端末と接続されている。ＬＡＮインターフェイス回路３７は、周知のバス型ＬＡＮとの信号のインターフェイス機能を有し、ＣＰＵ３３の制御に基づき他のＬＡＮ宛のＬＡＮパケットを受信してＲＡＭ３５内の送信バッファに格納する。また、受信／復号され、ＲＡＭ３５内の受信バッファに蓄積されている自ＬＡＮ宛のＬＡＮパケットをＬＡＮに送信する。

【０００９】ＣＰＵ３３はＲＯＭ３４に格納されたプログラムに基づき無線伝送装置全体を制御する。即ち、送信バッファ内のＬＡＮパケットを、共通鍵情報に基づいて暗号化し、伝送用に符号化してインターフェイス回路３２を介して出力する。また、受信データを伝送符号を復号化し、更に暗号の復号化を行って、ＬＡＮパケットを再生してＲＡＭ３５内の受信バッファに格納する。受信データに誤りが検出された場合には、ＣＰＵ３３は相手装置に対して再送要求パケットを送信し、再送要求パケットを受信した相手装置は保存してある送信パケットを再送する。ＲＯＭ３４の少なくとも一部は例えばフラッシュメモリのような電気的に消去、書き込みが可能な構成となっており、この部分に共通鍵情報が書き込まれ、保存される。

【００１０】送受信回路３１は送信回路および受信回路を内蔵し、送信回路は入力されたデータに基づきキャリアを変調し、所定の周波数帯域へ変換し、増幅して出力する。変調方式はＱＡＭなど任意であり、帯域も任意である。また、スペクトラム拡散方式を採用してもよい。送信信号はアンテナ３０から送信される。送受信回路２６～２９の受信回路は、アンテナ３０から受信した信号を復調し、復号して出力する。なお、送信回路と受信回路とは例えば減衰器を介して接続されているが、送信電力が数ミリワット程度であり、かつ送信と受信を交互に行う半二重通信を行うのであれば問題はない。

【００１１】パネル回路３６は例えばＤＩＰスイッチおよび発光ダイオードからなる簡単な入出力用のパネル回路であり、ＤＩＰスイッチの状態はＣＰＵ３３によって例えば周期的に読み取られ、また装置の状態が発光ダイオードに表示される。ＤＩＰスイッチの内の１つは、無線伝送装置の共通鍵設定モードを起動するために使用され、他の１つは無線伝送装置を親局として動作させるかあるいは子局として動作させるかを指定するために使用される。

【００１２】図４は、本発明の無線伝送装置の共通鍵設定処理の内容を示すフローチャートである。この処理は例えばタイマによって周期的に起動される。Ｓ１０においては、前記した共通鍵設定モードを起動するためのＤＩＰスイッチがオンであるか否かが判定され、判定結果が肯定の場合にはＳ１１に移行する。Ｓ１１においては無線伝送装置を親局として動作させるかあるいは子局として動作させるかを指定するために使用されるＤＩＰスイッチの設定が親局になっているか否かが判定され、判定結果が肯定である場合にはＳ１２に移行するが、否定の場合にはＳ１５に移行する。

【００１３】設定が親局の場合、Ｓ１２においては、例えば起動する度にランダムな値を発生する周知のプログラムを使用して例えば６４ビットのランダムな共通鍵情報を生成する。Ｓ１３においては、生成した鍵情報を前記した電気的書き込み可能な不揮発性ＲＯＭに書き込んで保存する。Ｓ１４においては、生成した鍵情報を所定のユニークなフォーマットでＬＡＮポートから送信する。

【００１４】設定が子局の場合、Ｓ１５においては、ＬＡＮポートから鍵情報が格納されたユニークなフォーマットのＬＡＮパケットが受信されるまで待ち、Ｓ１６においては、受信した鍵情報を前記した書き込み可能な不揮発性ＲＯＭに書き込んで保存する。Ｓ１７においては前記した共通鍵設定モードを起動するためのＤＩＰスイッチがオフになるまで待ち、処理を終了する。

【００１５】次に、図２を参照して、共通鍵の設定方法について説明する。まず、共通鍵を設定すべき無線伝送装置２０～２２全部のＬＡＮポートをハブ２５へ接続する。次に、無線伝送装置２０～２２の内の１台のみについて、パネル回路３６内の無線伝送装置を親局として動作させるかあるいは子局として動作させるかを指定するためのＤＩＰスイッチを「親局」に設定する。そして、その他の無線伝送装置２１、２２の該ＤＩＰスイッチを「子局」に設定する。

【００１６】次に、「子局」に設定した無線伝送装置２１、２２の共通鍵設定モードを起動するためのＤＩＰスイッチをオンにする。これで、「子局」の無線伝送装置は図４のＳ１５の待機状態となる。最後に、「親局」に設定した無線伝送装置２０の共通鍵設定モードを起動するためのＤＩＰスイッチをオンにする。この操作により、「親局」の無線伝送装置２０は図４のＳ１２～１４の処理を実行して、共通鍵を生成し、保存すると共に子局へ転送し、子局においては、鍵情報を受信して格納する。

【００１７】以上のような構成および動作によって、全ての無線伝送装置に、使用者のみならず管理者や保守者にも開示されることなく、秘密の共通鍵情報を設定することができる。なお、本発明の共通鍵設定方法においては、全ての無線伝送装置において共通鍵設定モードを起動しないと、共通鍵の設定が行えない。従って、例えば親局に設定した無線伝送装置にのみ施錠等の管理を行うことにより、前記ＤＩＰスイッチへのアクセスを禁止すれば、子局の無線伝送装置については特に対策を施さなくても鍵の変更を防止することが可能である。

【００１８】以上、本発明の実施例を開示したが、本発明には下記のような変形例も考えられる。実施例においては、通信に使用するＬＡＮポートを利用して共通鍵の設定を行う例を開示したが、共通鍵の設定処理用に専用の例えばRS-232Cなどの有線接続ポートを設けてもよい。この場合、無線伝送装置が端末機能を有していれば、ＬＡＮポートは不要の場合もある。また、無線伝送装置は無線リンクを具備しているので、該無線リンクを共通鍵設定処理に使用してもよい。

【００１９】前記したように、親局のみを管理すれば不正な設定は防止可能であるので、例えば親局に、図４のＳ１４のみを実行する共通鍵コピー機能を備えてもよい。この場合には、例えば増設する子局の無線伝送装置と親局の無線伝送装置とをハブで接続し、子局の共通鍵設定モードを起動しておいて、親局において前記した共通鍵コピー処理を起動する。すると、親局から子局に共通鍵が送信され、子局に共通鍵が格納される。以上の処理によって、無線伝送装置を増設する場合に全ての無線伝送装置をハブで接続する必要が無くなる。

【００２０】なお、上記のようなコピー機能を設けた場合、子局のＤＩＰスイッチを変更して親局とし、コピー機能を使用して共通鍵を読み出すことも考えられる。従って、例えば共通鍵の格納エリアに現在の親／子設定情報も格納しておき、子局から親局に設定が変更された場合には、格納されている共通鍵を消去するなどの対策をとっておく。

【００２１】

【発明の効果】以上述べたように、本発明においては、無線伝送装置において、鍵設定モード起動手段によって鍵設定モードが起動された場合に、親／子指定手段により親局に指定されている場合には、鍵生成手段によって鍵を自動的に生成し、鍵記憶手段によって鍵を不揮発性の記憶手段に格納すると共に、鍵転送手段によって鍵を他の無線伝送装置に転送し、子局に指定されている場合には、鍵受信手段によって鍵を受信し、鍵記憶手段によって鍵を不揮発性の記憶手段に格納するように構成したので、例えばシステムのセッティングを行う業者でさえも設定される鍵情報を知ることができず、機密性が向上するという効果がある。

【００２２】また、本発明によれば、共通鍵を設定する場合には設定すべき無線伝送装置をＬＡＮ等によって有線接続する必要があるので、職場等に設置した後に例えば盗聴しようとする者が共通鍵設定処理を実行することが困難となるという効果もある。更に、子局を増設する場合などには全ての無線伝送装置において共通鍵設定処理をやり直し、新たな鍵情報が設定されるので、使用者が鍵の解読を試みることも困難であり、鍵が解読される恐れが減少するという効果がある。

【図面の簡単な説明】

【図１】本発明を適用した無線伝送装置を含む通信システムの構成を示すブロック図である。

【図２】本発明の共通鍵設定処理を実行するためのシステム構成を示すブロック図である。

【図３】本発明の無線伝送装置の構成を示すブロック図である。

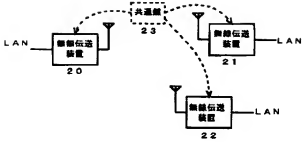
【図４】本発明の無線伝送装置の共通鍵設定処理の内容を示すフローチャートである。

【図５】従来の無線伝送装置における共通鍵設定方法を示すブロック図である。

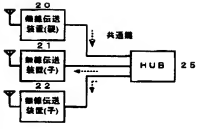
【符号の説明】

１０、１１、１２…無線伝送装置、１３…端末、２０、２１、２２…無線伝送装置、２３…共通鍵情報、２５…ハブ、３０…アンテナ、３１…送受信回路、３２…インターフェイス回路、３３…ＣＰＵ、３４…ＲＯＭ、３５…ＲＡＭ、３６…パネル回路、３７…ＬＡＮインターフェイス回路

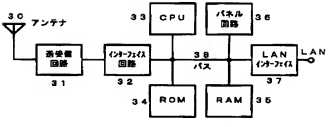
【図1】


共通鍵
23
LAN
無線伝送装置
20
無線伝送装置
21
LAN
無線伝送装置
22
LAN

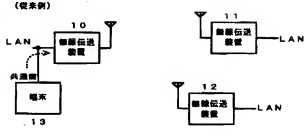
【図2】


20
無線伝送装置(親)
共通鍵
21
無線伝送装置(子)
HUB
25
22
無線伝送装置(子)

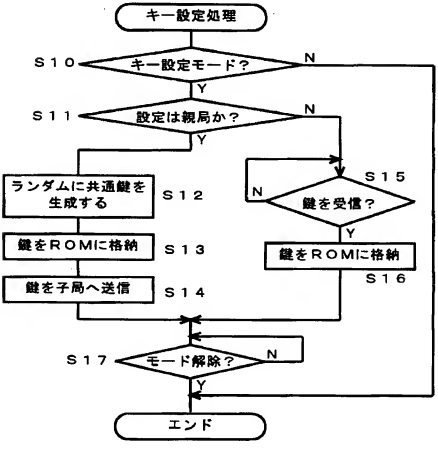
【図3】


30
アンテナ
33
CPU
パネル回路
36
送受信回路
31
インターフェイス回路
32
38
バス
LAN インターフェイス
37
LAN
34
ROM
RAM
35

【図5】


(従来例)
10
LAN
無線伝送装置
共通鍵
端末
13
11
無線伝送装置
LAN
12
無線伝送装置
LAN

【図4】


キー設定処理
S10
キー設定モード？
N
Y
S11
設定は親局か？
N
Y
ランダムに共通鍵を生成する
S12
鍵をROMに格納
S13
鍵を子局へ送信
S14
S15
N
鍵を受信？
Y
鍵をROMに格納
S16
S17
モード解除？
N
Y
エンド

【手続補正書】
【提出日】平成１２年３月９日（２０００．３．９）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】無線データ送受信手段と、鍵を不揮発性の記憶手段に格納する鍵記憶手段と、鍵を使用してデータの暗号化復号化を行う暗号化手段とを具備する無線伝送装置において、
鍵生成手段と、
鍵設定モード起動手段と、
親／子指定手段と、
無線伝送装置と端末装置との間でデータ伝送を行うための有線データ送受信手段と、
前記有線データ送受信手段を使用して鍵を他の無線伝送装置に転送する鍵転送手段と、
前記有線データ送受信手段を使用して鍵を受信する鍵受信手段と、
前記鍵設定モード起動手段によって鍵設定モードが起動された場合に、前記親／子指定手段により親局に指定されている場合には、前記鍵生成手段によって鍵を生成し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納すると共に、前記鍵転送手段によって鍵を他の無線伝送装置に転送し、前記親／子指定手段により子局に指定されている場合には、前記鍵受信手段によって鍵を受信し、前記鍵記憶手段によって鍵を不揮発性の記憶手段に格納する鍵設定制御手段とを備え、
更に、前記親／子指定手段により親局に指定されている場合に、前記不揮発性の記憶手段に格納されている鍵を前記鍵転送手段によって他の無線伝送装置に転送する鍵コピー手段を備えたことを特徴とする無線伝送装置。
【請求項２】更に、子局に指定されていた無線伝送装置が親局に指定された場合には、前記不揮発性の記憶手段に格納されている鍵を消去する鍵消去手段を備えたことを特徴とする請求項１に記載の無線伝送装置。

拒絶査定

特許出願の番号	特願２００３－１０８２７６
起案日	平成１９年　５月１４日
特許庁審査官	土居　仁士　　９３７１　５Ｘ００
発明の名称	情報通信システムおよび方法、情報通信装置および方法、プログラム
特許出願人	ソニー株式会社
代理人	稲本　義雄

この出願については、平成１８年１１月１３日付け拒絶理由通知書に記載した理由によって、拒絶をすべきものである。
なお、意見書及び手続補正書の内容を検討したが、拒絶理由を覆すに足りる根拠が見いだせない。

備考
出願人は、手続補正書を提出することにより特許請求の範囲を補正するとともに、意見書において、「引用文献１には、２台の携帯型情報端末が、一対一で接続して、無線設定情報を取得することのみが単に開示されているだけであり、有線ネットワークに複数の情報通信装置が接続され得る環境での無線設定情報の取得については、開示は勿論示唆もされていません。」旨主張している。
しかしながら、無線で利用するパラメータを直接接続やＬＡＮ等による有線接続で送付すること、また、送付を物理的に設けたトリガにより開始することは、例えば特開２０００－３４１２６２号公報に記載されるように周知技術であるから、補正後の請求項１乃至２６に係る発明は、出願人の意見書における主張にかかわらず、依然として当業者が引用文献１に記載された発明および周知技術から容易になし得たことであると認められる。

この査定に不服があるときは、この査定の謄本の送達があった日から３０日以内（在外者にあっては、９０日以内）に、特許庁長官に対して、審判を請求することができます（特許法第１２１条第１項）。
（行政事件訴訟法第４６条第２項に基づく教示）
この査定に対しては、この査定についての審判請求に対する審決に対してのみ取消訴訟を提起することができます（特許法第１７８条第６項）。

部長／代理	審査長／代理	審査官	審査官補
	宮島　郁美	土居　仁士	
	８５２３	９３７１	